MALICIOUS

Classifications: -

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Word Document**
File Name	**9cb01729327bd958e32aa9481d5a81303627ab7a59b9ae134fb6600ef4e5b680.doc**
ID	#5127352
MD5	cadb9d5ed47b8df81a2addefed302a03
SHA1	f7197fa991510f99f25af2b502c40d3b48d1abbc
SHA256	9cb01729327bd958e32aa9481d5a81303627ab7a59b9ae134fb6600ef4e5b680
File Size	2262.21 KB
Report Created	2022-08-11 20:42 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (5 rules, 5 matches)

Score	Category	Operation	Count	Classification
4/5	Network Connection	Attempts to connect through HTTP	1	-
	• (Process #1) winword.exe failed to connect to http://45.8.146.139/fhfty/SKWR8YXON-RX9R4781JWMO3UUH0NGDBO/-f.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
3/5	Network Connection	All network connection attempts failed	1	-
	• Host "45.8.146.139" is unavailable.			
2/5	Execution	Executes macro on specific event	1	-
	• Executes macro automatically on target "document" and event "open".			
1/5	Execution	Contains suspicious Office macro	1	-
	• Office document contains a suspicious VBA macro.			

Mitre ATT&CK Matrix

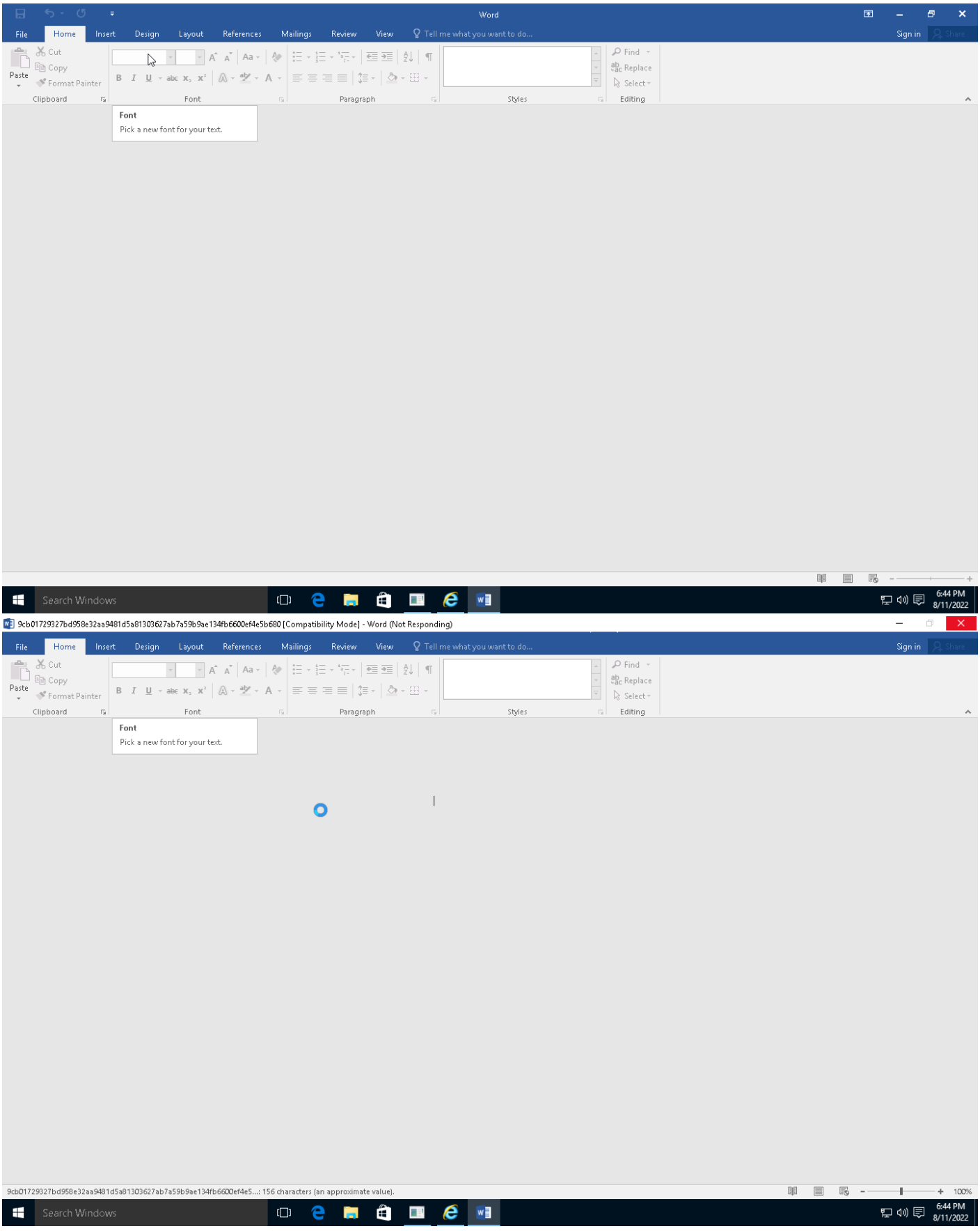
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1064 Scripting			#T1064 Scripting					#T1071 Standard Application Layer Protocol		

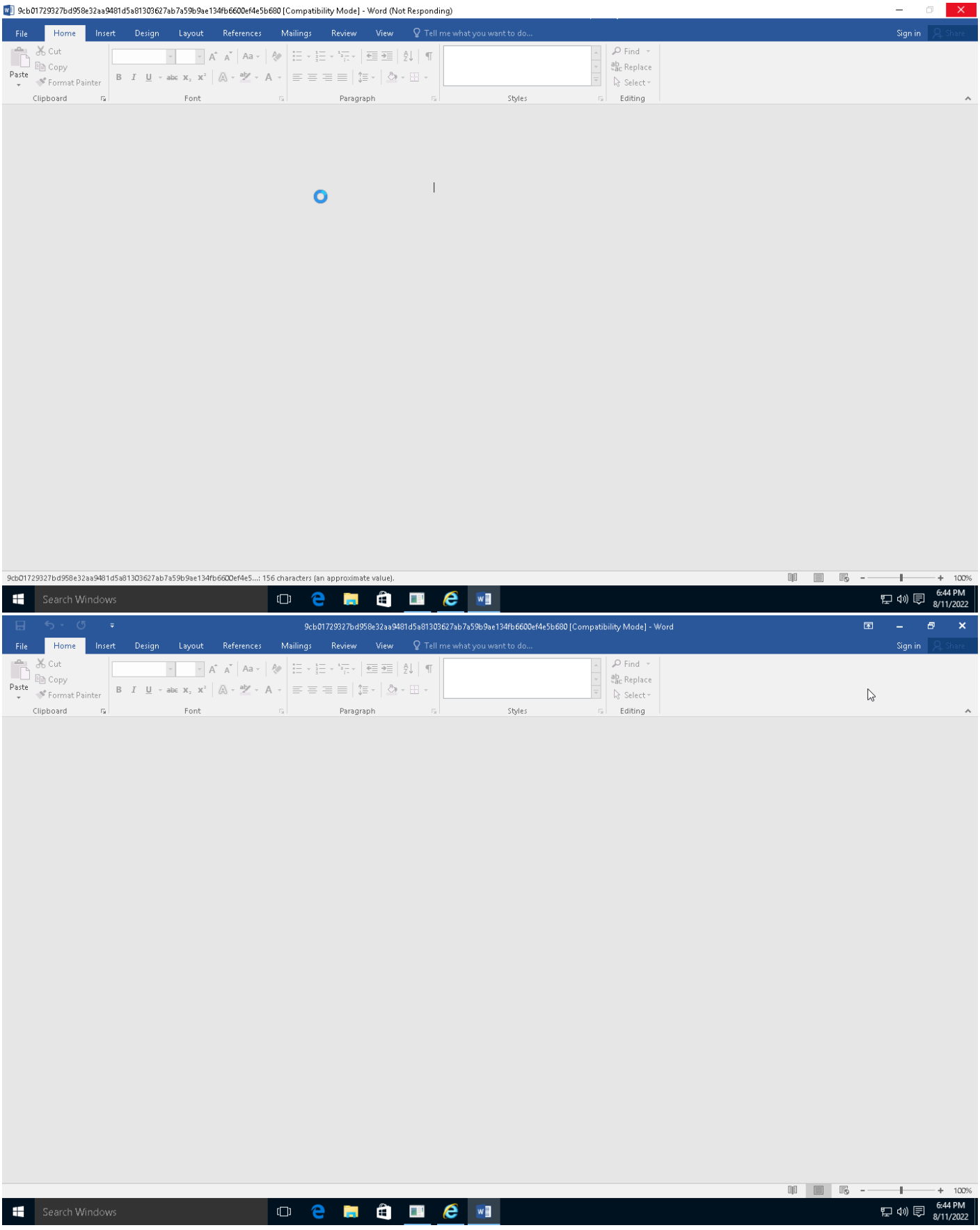
Sample Information

ID	#5127352
MD5	cadb9d5ed47b8df81a2addefed302a03
SHA1	f7197fa991510f99f25af2b502c40d3b48d1abbc
SHA256	9cb01729327bd958e32aa9481d5a81303627ab7a59b9ae134fb6600ef4e5b680
SSDeep	49152:7t3L6IYFlSbzCFelOb0h5CZTsXG97qRbET6DLZ6dGbrG5j:BPYYgelO9T6G97qVg6DLZ6dGbyh
File Name	9cb01729327bd958e32aa9481d5a81303627ab7a59b9ae134fb6600ef4e5b680.doc
File Size	2262.21 KB
Sample Type	Word Document
Has Macros	✔

Analysis Information

Creation Time	2022-08-11 20:42 (UTC+2)
Analysis Duration	00:04:06
Termination Reason	Timeout
Number of Monitored Processes	1
Execution Successful	False
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Word
File Home Insert Design Layout References Mailings Review View Tell me what you want to do... Sign in Share
Paste Cut Copy Format Painter
Clipboard Font Paragraph Styles Editing
Find Replace Select
Font
Pick a new font for your text.
Search Windows
6:44 PM
8/11/2022
9cb01729327bd958e32aa9481d5a81303627ab7a59b9ae134fb6600ef4e5b680 [Compatibility Mode] - Word (Not Responding)
9cb01729327bd958e32aa9481d5a81303627ab7a59b9ae134fb6600ef4e5...: 156 characters (an approximate value).
100%



Screenshots truncated

NETWORK

General

152 bytes total sent

0 bytes total received

1 ports 80

1 contacted IP addresses

1 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://45.8.146.139/fhfty/SKWR8YXON-RX9R4781JWMO3UUH0NGDBO/-f	-	-		0 bytes	NA

BEHAVIOR

Process Graph

Process #1: winword.exe

ID	1
File Name	c:\program files (x86)\microsoft office\office16\winword.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 62614, Reason: Analysis Target
Unmonitor End Time	End Time: 309541, Reason: Terminated by timeout
Monitor duration	246.93s
Return Code	Unknown
PID	4840
Parent PID	1972
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\yCB9A.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	84
Keyboard	52
System	10
File	7
Environment	1
-	4

Network Behavior

Type	Count
HTTP	1
TCP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9cb01729327bd958e32aa9481d5a81303627ab7a59b9ae134fb6600ef4e5b680	C:\Users\RDhJ0CNFevzX\Desktop\9cb01729327bd958e32aa9481d5a81303627ab7a59b9ae134fb6600ef4e5b680.doc	Sample File	2262.21 KB	application/vnd.openxmlformats-officedocument.wordprocessingml.document	-	MALICIOUS
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	-	Modified File	128 bytes	application/octet-stream	-	CLEAN
f259cd4e253fe1a21165fa3c903165ea987af6980ff252268c23c4dab2176786	image2.png	Extracted File	249.85 KB	image/png	-	CLEAN
0d79507fbc5d3c1843f0584e92ffd8b8f2862b4ae569beb934963b30185e6489	image1.png	Extracted File	77.99 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\9cb01729327bd958e32aa9481d5a81303627ab7a59b9ae134fb6600ef4e5b680.doc	Sample File, VM File	-	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\yCB9A.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN
image2.png	-	-	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\yCB9A.tmp.dll	Accessed File	Access, Create	CLEAN
ThisDocument	-	-	CLEAN
image1.png	-	-	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://45.8.146.139/fhfty/SKWR8YXON-RX9R4781JWMO3UUH0NGDBO/-f	-	45.8.146.139	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
45.8.146.139	-	Russia	TCP	SUSPICIOUS

Process

Process Name	Commandline	Verdict
winword.exe	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.12 / 2022-08-02 11:53:09
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.16 / 2022-08-10 15:34:29
YARA Built-in Ruleset Version	4.6.1.10

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp

System Root	C:\Windows